The Attorney General's Special Report on Medical Record Confidentiality

Scott Harshbarger
Attorney General
Commonwealth of Massachusetts

May 1998

TABLE OF CONTENTS

I.

Introduction

From the days of Hippocrates to the present, people seeking medical care have acted on the automatic assumption that a patient's communication with a doctor is confidential. The common understanding that people need to feel free to confide their most intimate, embarrassing, shameful or tragic concerns to their doctors without fear of disclosure, in order to obtain complete and appropriate treatment, has been an unquestioned premise of good medical practice for centuries. Until relatively recently, this confidence in doctor-patient secrecy has, for the most part, been justified. Massachusetts in particular has long and rightly been considered at the forefront in providing legal protection to its citizens' medical confidences. However, the avalanche of changes that has overtaken the practice of medicine in the past fifteen years (including the introduction of managed care, the information technology revolution, mergers and consolidations of health care providers, direct marketing of medical treatments and drugs to consumers and the increased understanding and value of genetic information) has affected medical confidentiality as well. Unknown to the general public, which has largely continued to believe that all that is said or done within the walls of a doctor's office will remain there unless they consent to its disclosure, the confidentiality of medical information has begun to fray badly at the edges. While the laws of the Commonwealth were once more protective than most, and the record of health care providers in maintaining confidentiality has, for the most part, been excellent, changing times have left the law insufficient to maintain privacy in the face of advancing technology and increased demands for access from non-providers, such as insurance and pharmaceutical companies.

As the Attorney General has a constitutional and statutory mandate to protect both the civil rights and the consumer rights of the citizens of Massachusetts, he has a unique interest in assuring that the protection for privacy keeps pace with the encroachments. In the past two years those encroachments have become increasingly apparent. The following are some of the situations that have come to the attention of the Attorney General and have triggered this review:

1. In 1995, public attention focussed on the Commonwealth's largest health maintenance organizations as a result of press reports that it integrated patients' mental health records, including detailed notes of clinical encounters, with the general health records of the patient. Because the HMO maintained its records on an organizational intra-net, the comprehensive health record was readily available to anyone in the organization with access to a computer at any of the health centers. While it was the expanded access to mental health data that caused the strongest reaction by the public, the press reports were also the first time public attention was drawn to the fact that the paper records formerly maintained by the HMO were being moved into a computer data base, raising issues of consent, and the security of the information during the transfer.

2. In 1996 an employee of a major Massachusetts hospital used a former employee's top-level clearance code repeatedly over a four month period to access all the computerized medical records of the hospital, and then made obscene phone calls to young female patients whose records he had read. The crime was possible because the hospital had not automatically cancelled the password of the former employee. It was also more difficult to track down the trespasser in the system because the hospital apparently had no method of auditing access to individual patient files.

3. Repeatedly, residents of the Commonwealth have written to the Attorney General to complain that, shortly after being diagnosed with a specific medical condition (allergies, prostate problems) they have received direct mail solicitations from drug companies to buy medications for treatment of the condition. This has raised the concern that medical confidentiality was breached in the sale of mailing lists to advertisers. Most recently, published reports that a major chain of pharmacies was using its access to prescription information for marketing purposes has added to this concern.

4. Particularly with regard to accessing mental health care, but in other situations as well, consumers have complained of being asked to provide extensive confidential information to non-clinicians when phoning to get authorization for the care, or to make appointments with care providers. In some cases, the persons asking for the information identify themselves as "medical assistants" which may mislead patients into believing they are speaking to a medically trained professional, rather than a clerically trained receptionist. While there are circumstances where administrative personnel must have access to medical information, consumers should be aware of who they are speaking with, particularly when they are asked to divulge medical confidences.

5. Some consumers have complained of indiscriminate distribution of their medical information within their HMO care group, e.g. coming in for a one-time visit to a dermatologist for a minor problem and finding the doctor in possession of their entire medical record.

6. Some clinicians have complained that health insurers ask them to collect and provide more information, in greater detail than they considered appropriate, from the patients in order to be certified for reimbursement by the companies. For example, the Attorney General has received a complaint that, after a doctor had made a diagnosis based on what the doctor believed to be adequate clinical data, the insurer demanded a confirming x-ray. Although the doctor did not believe the x-ray was necessary, and the patient did not want unnecessary exposure to radiation, the insurance company refused to reimburse for the treatment unless the x-ray was provided. This raises concerns as to both the patient's privacy as well as the issue of who is directing the patient's care.

7. As the scientists engaged in figuring out the complete human genetic code make more and more progress toward a complete genetic "map," more information becomes available regarding the function and use of genetic material. As a result, civil rights advocates have begun raising questions about the ownership and use of individual genes, and about the rights of citizens who have been tested for genetic defects. There have been complaints from individuals who have lost jobs or insurance after learning of a genetic predisposition to certain diseases. Also, now that the U.S. Supreme Court has ruled that altered genes are patentable property, the increased value of human genetic material also raises consumer protection issues.

8. Beginning with both the failed attempt at establishing national health insurance, and with the "Medical Record Confidentiality Act of 1995," (also known as the "Bennett Bill") which also failed to pass, Congress has begun to debate the federal regulation of medical information. In 1996, Congress passed the "Health Insurance Portability and Accountability Act of 1995" (also known as the "Kassebaum-Kennedy Act"or "HIPAA") which, among other things, mandates the development of industry-wide standards for a "universal patient identifier" to be used throughout the health care system. This "UPI" may eventually also have the potential to link identified individuals with non-medical information databases (i.e. financial or law enforcement). The trend towards diminishing privacy rights in the federal sector is of concern to the Attorney General, particularly as the less stringent federal standards on privacy may pre-empt more protective state laws if federal law is not carefully drawn to protect state standards.

9. Recently, the Group Insurance Commission of the Commonwealth , a state agency responsible for negotiating and purchasing group health insurance policies for state employees, was sued for allegedly releasing confidential medical information to private entities in violation of state privacy laws. Regardless of the merit of the allegations, which the Commission denies, the case raises questions as to the access state officials have to individual medical records, and the statutory basis for disseminating records for research and quality review purposes.

In light of the various concerns raised by the above list, the Attorney General has assessed the current state of the law protecting medical privacy, as balanced against certain basic principles defined below. In this report he provides his conclusions and recommendations in furtherance of the public interest.[1]

II.

The Importance of Medical Record Confidentiality

For the purpose of this review, the Attorney General concurs with and has adopted the set of basic principles shared by the American Medical Association ["Principles of Medical Ethics, Code of Professional Responsibility," Garlin ed. 1986] and the Massachusetts Medical Society as embodied in its recently adopted "Policy on Patient Privacy and Confidentiality," November 8, 1996.

Three fundamental elements underlie the principles:

(1) There is a basic right of patients to the privacy of their medical information and records;

(2) Privacy should be maintained and respected unless it is waived by the patient in a meaningful, informed and non-coerced way, except in the rare and carefully defined case where public interest requires otherwise;

(3) Even in the case of consented-to disclosure, only information necessary to the particular use and no more should be disclosed.

Medical information is different from any other kind of information that an individual can disclose about herself. Unlike financial information, inappropriate dissemination of some medical information has the capacity to destroy the life of the person whose privacy is violated.

The Attorney General is unfortunately well aware of discrimination in housing and employment and public accommodations that comes when a HIV+ status or treatment for mental illness or drug dependency is revealed. His office has been called upon to protect women who become the targets of threats and harassment when it became known that they had abortions. He is aware of child custody cases that turned on the unauthorized disclosure of the medical history of one of the parents. He has discussed with civil rights advocates the growing concerns around genetic discrimination. It has always been a most powerful argument for medical privacy that its loss can result in the loss of other fundamental rights.

But in addition to issues of major sensitivity, even relatively minor breaches of medical privacy can do serious harm to the person exposed. While revelations of such major diagnoses as positive HIV status or schizophrenia can turn an individual into an object of fear and hatred, revelations of the other kind can turn him into a laughingstock.

Because protecting medical privacy is essential to the protection of basic human dignity, it follows that, except in extraordinary circumstances, only the individual should decide when and how to relinquish it. While many of the current threats to medical privacy arise from benign motives, others do not. It is true that computerization and network of

medical records offers improved care to patients, a doctor who has all her patients' records on computer can easily track immunization schedules for example, and can quickly retrieve and review relevant history when a patient telephones or comes in for a specific problem. Moreover, she saves time, which both reduces the costs and makes her more available to provide treatment. If her records are networked with a hospital, she can save a patient valuable time in the event of an emergency admission. From a patient care perspective, there are many reasons why a properly managed computerized record can be a benefit. Permitting one's records to be networked may be worth the risk to privacy from making one's records more accessible, provided appropriate security is in place. The protection necessary in this context is technological: adequate training, multi-level access programs, password protections, limitations on altering the data, electronic signatures, etc.

However, the risk-benefit analysis will change significantly for most people when the threat to their privacy comes, not from care givers, but from "secondary users." Insurance companies, researchers, public health agencies, litigators and investigators, managed care companies and marketing entities all collect health data in ways that do not always respect patient privacy and interests. Health data is becoming a valuable asset in and of itself and the temptation to limit or even dismiss privacy protection is great. In fact, it is the secondary users, particularly the federal government, driven by cost containment and/or research concerns, that appear to be most in favor of loading all medical information into linked national databases, with universal patient identifiers for each individual. In the medical context, this is a disturbing trend, for the easier access to this information, the more likely it is to be both used and abused.

As can be seen in the following section, current law in Massachusetts no longer stands at the forefront of medical privacy protection. In today's high tech environment and in the face of increasing interest in the data, it provides only minimal protection and, in many crucial areas, none at all.

III.

The Current State of the Law Governing Medical Record Privacy in Massachusetts

A. All Medical Care Providers are Obligated To Collect and Maintain Medical Information

All providers of medical services maintain records on each contact with a patient . The records are intended generally to serve three basic purposes: (1) to record and communicate necessary information to all who are involved in a patient's care, either at the time or in the future; (2) to create a legal document for the purpose of establishing that relevant standards of care were met by the treatment, and (3) to satisfy various statutory and regulatory requirements. Medical records must at the very least contain sufficient information to identify a patient, support the diagnosis, and explain and document the course and results of the treatment prescribed.

In Massachusetts, hospitals or clinics licensed by the Department of Public Health, or funded in whole or in part by the Commonwealth, keep records of the treatment of cases under their care and to maintain them for thirty years. [2] The specifics of the information to be collected and maintained has been defined by the American Medical Association Council on Standards and the Joint Commission on the Accreditation of Health Organizations (JCAHO) for its accredited facilities as including:

1. identifying information
2. demographic information, including legal status
3. medical history
4. results of each physical examination, including chief complaint, details of present illness, relevant past social and family history, and inventory of body systems.
5. tests and therapies ordered
6. emergency treatment
7. reasons for treatment/admission
8. progress notes
9. consultation reports
10. medications ordered and administered.
11. in obstetrical cases, pre-natal information
12. consents

As western medical practice becomes more alert to the interaction between physical and mental health, and the significance of environmental factors in the cause and treatment of physical disorders, medical care providers are starting to collect and record information that can also relate to financial and social status in greater detail. Moreover, there are numerous requirements for medical care providers to collect specific information

from their encounters with patients (See Required Disclosure/Mandated Reporting, below). It is safe to say that most individuals would be surprised at the breadth and depth of the information to be found in the standard medical record.

Medical records are the physical property of the hospital or the physician practice that created them and there is no obligation to surrender the original record to a patient. Given the various legal obligations on care providers to keep and maintain these records, it would take extraordinary circumstances for a patient to have the right to claim the original records. Copies, however, must be made available. Patient access to their records is discussed under (C) below.

B. Physicians Have An Obligation To Keep Patient Communication Confidential

Most people are probably familiar with the concept of "doctor patient" privilege, and believe it to mean that communications with a doctor may never be revealed, in or out of court, unless the patient consents. Generally speaking, this is not an accurate understanding of the doctor's obligation to respect patient confidences. While doctors are ethically bound to maintain patient confidences by the Hippocratic Oath, Massachusetts does not have a statute making physician-patient communication privileged. Therefore, the legal limits of doctor-patient confidentiality have been defined by the courts, which have recognized the physician's general obligation to keep patient communication confidential, but with some exceptions.[3] The Supreme Judicial Court, citing to the Hippocratic Oath, has held that out-of-court disclosure of patient information can give rise to a cause of action for damages against a physician, except where "compelling circumstances justify disclosure to a person with a legitimate interest in the person's health."[4] "[A]ll physicians owe their patients a duty, for violation of which the law provides a remedy, not to disclose without the patient's consent medical information about the patient except to meet a serious danger to the patient or to others." [5]In the commonwealth, physicians have ethical, common law and, in some cases, contractual obligations to maintain confidentiality, and may be subject to an action in tort or contract as appropriate, for damages.[6]

Furthermore, the Massachusetts' "Patient's Bill of Rights"[7] enacted in 1979, provides that patients in defined health care settings[8] "have the right to confidentiality of all records and communications to the extent provided by law." In addition, patients can put certain limits on the information collected about them, as they have the right to refuse to serve as research subjects, or to refuse an examination when the primary purpose of the examination is educational for the doctor, rather than therapeutic for the patient. Violation of the statute can give rise to a claim of malpractice.[9] [10] [See also, Other Protections of Privacy, below, for other statutory claims as well.]

C. Patient Access to Collected Information

Medical records of patients in a Department of Public Health licensed facility (or other facility licensed by the commonwealth) may be inspected by the patient, the patient's attorney with written authorization from the patient, or the legal representative of a deceased patient's estate. Copies must be furnished for a "reasonable fee," unless the records are needed to apply for a needs-based benefits program, in which case the record must be copied without charge to the patient.[11]

Patients in a facility licensed by the Department of Mental Health may obtain records in the same manner as patients in a DPH-licensed facility, unless the records were created by a mental health practitioner who believes that disclosure of the record would not be in the best interests of the patient. In those cases, disclosure will be made to another mental health practitioner chosen by the patient, but not to the patient directly.

Patients in facilities listed in the "Patient's Bill of Rights" may also inspect records and receive copies.[12] There is no specific provision in state law for patients to object to , or change entries in their medical records. However, under state law, a patient is entitled "to have all reasonable requests responded to promptly and adequately within the capacity of the facility." This could presumably include a request for a change in the record, or for inclusion in the record of a patient statement for records held by covered facilities. [13] As to records maintained by individual physicians and other health care providers, patients or authorized representatives are entitled to inspect the records, and receive copies for a "reasonable fee."[14]

Parents, including non-custodial parents, may access the medical records of their minor children, except that the record of a minor's court-authorized abortion may not be disclosed without her written consent.[15]

Health care agents acting pursuant to a valid proxy may, after a determination that the health care principal is incompetent, access the principal's medical record.[16]

There are no laws or regulations governing access to information filed with, but not considered a part of, the medical record, such as correspondence, or administrative records (e.g. audit trails) or records from other institutions.

D. Disclosure With Consent

As a general principle, any disclosure of a medical record is lawful if made with the consent of the person who is the subject of the record. In addition, custodial parents may consent to the disclosure of a child's medical record and guardians may consent on behalf of the person they represent. Emancipated minors may consent on their own behalf.[17]

A health care agent, acting pursuant to a valid proxy may, after a determination is made that the health care principal is incompetent, consent to disclosure of the principal's records.[18]

The results of a test for HTLV-III may only be disclosed with specific written consent by the patient and an individual consent is required for each disclosure.[19] However, under pending legislation, the consent requirement would be waived if the patient seeks to sell his or her life insurance benefits; potential purchasers would be entitled to access this information without consent.[20]

It should be noted that a "consented to" disclosure may not be a "voluntary" disclosure; if a patient cannot access necessary care without providing consent, the consent is not optional.

E. Required Disclosure/Mandated Reporting

There are many circumstances under which identifiable medical information may be released by a health care provider without the consent of the patient and, in many cases, without the patient's knowledge. As an initial premise, nearly every statute which purports to protect the privacy of medical records allows for disclosure "as authorized by law" and there are an increasing number of those authorizations. The following are state-law authorized exceptions to confidentiality of medical information by law:[21]

- A hospital or clinic served with a subpoena for the records of a party named in the case must deliver the records to a court or designated place of hearing, including a deposition.[22]

- The Commissioner of the Department of Mental Health has the authority to permit inspection and/or disclosure of medical records of a facility within the department's jurisdiction where the Commissioner determines it would be "in the best interest of the patient or resident."[23] The statute governs patient records of the department "notwithstanding any other provisions of the law."

- The Commissioner of the Department of Public Health may similarly authorize the release of medical records within his jurisdiction without patient consent, and there is no requirement that the disclosure be in the best interest of the patient.[24]

- The Commissioner of Public Health may authorize "scientific studies and research which have for their purpose the reduction of morbidity and mortality within the Commonwealth."[25] Anyone submitting information for an authorized study "shall not [be] subject to any action for damages or other relief." Information, including medical record information, submitted to the department or any person, agency or organization carrying out authorized research must be kept confidential by anyone having access to the information in connection with the study; the penalty for disclosure is a fifty dollar fine.

- If a patient reports an injury to a physician which appears to be eligible for worker's compensation, the medical report pertaining to the injury "shall be furnished by the physician, or other medical provider to the employee, the insurer and the department [of Industrial Accidents] within 14 days of the examination."[26] There is no provision for patient consent and a failure to report is punishable by a civil fine of between $25-$1000.[27] However, in practice medical record holders will obtain consent prior to release of these records, on the assumption that this statute does not provide an exemption from privacy protections of other statutes governing release of medical records.

- There are multiple statutes requiring medical care providers to disclose specific types of medical information to public health authorities and, in some cases, to law enforcement, for the protection of the public. These include:

1. Infectious diseases or diseases declared by DPH to be dangerous to the public.[28]
2. Gunshot and knife wounds and burns.[29]
3. Suspected abuse or neglect of children.[30]
4. Suspected abuse or neglect of elders. A state-appointed ombudsman may also access the medical records of any mentally incompetent elder with no next-of-kin for the purpose of investigating abuse claims.[31]
5. Suspected abuse of a disabled person.[32]
6. Cancer registry.[33]
7. High risk infants.[34]
8. Live births.[35]
9. Deaths.[36]
10. Fetal deaths.[37]
11. Reyes Syndrome.[38]
12. Cerebral palsy.[39]
13. Lead poisoning.[40]
14. Abuse or neglect of nursing home residents.[41]

- Hospitals must notify pre-admission transporters (police officers, fire fighters, ambulance operators and attendants, EMTs, corrections officers) if a patient they have transported is subsequently diagnosed with an "infectious disease dangerous to the public health."[42] However, the patient identity should not be disclosed.

- If a person brings a lawsuit to recover for injuries where the hospital bill for treatment of the injuries was not covered by worker's compensation, the hospital may file a lien on the potential recovery, provided it gives notice of the lien to all parties to the lawsuit. Any party to the lawsuit may then request and receive an itemized list of the charges incurred by the patient.[43]

- If a health care provider releases medical information in connection with a patient's claim for benefits under a needs-based program, the provider is immune from liability for any claim by the patient, even if the patient did not consent to the disclosure.[44]

- The Commissioner of Public Health is authorized to create an advisory committee of six members to research and investigate degenerative diseases, including the autosomal dominant motor system diseases in persons of Portuguese ancestry.[45] The statute is silent on how the committee is to collect necessary medical information.

- If a person applies to the Division of Industrial Accidents for worker's compensation, the division may inspect all relevant medical records and those records are also open to any other party to the claim.[46]

Disclosure To And By Health Insurance Companies

Although most people believe that their consent is necessary for their health insurer to have access to their medical records, this is not actually the case. While many health insurers make formal consent to disclose a pre-requisite for enrolling in a health insurance program, state law does not require an applicant to give consent before an insurer may review a record. A unilateral statement in the insurance policy or certificate that access to the records is permitted is all the law requires in order for an insurer to review medical records.[47]

In addition, health care provider contracts with health insurers routinely require the doctor or other provider to make medical records of patients available for review upon request by the insurer.

Also, it should be noted that, even if a patient consents to an initial disclosure of medical information for a specific insurance purpose, there is no way to control its actual use. Once medical information is in an insurer's possession, it may be further disclosed for virtually any reason, as long as the disclosure can in some way be considered "reasonably

necessary" to perform a specific business, professional or insurance function or to detect or prevent criminal activity, fraud or material misrepresentation in connection with an insurance transaction, including but not limited to determining benefits, detecting criminal behavior or carrying out research.[48] It is this provision that allows release of medical record information to the central data base of the Medical Information Bureau.[49]

Finally, health care institutions may access medical records without consent for peer review and utilization review purposes.[50] Peer review committee records are confidential and a patient's medical record information, when obtained in connection with a peer review or utilization review, may not be introduced in evidence by the committee at any judicial or administrative proceeding except those held by the boards of registration in medicine, social work or psychology. [51] [52] However, submission of a patient's medical record information to the board does not exempt the information from being disclosed by the original custodian when otherwise appropriate in connection with an administrative or judicial proceeding.

Medical information and records, and other information submitted to a "risk management and quality assurance program" established by a hospital pursuant to the regulations of the board, are "deemed to be records of a medical peer review committee for the purposes of section 204" and are confidential to the same extent, as long as the records are "necessary to comply with risk management and quality assurance programs."[53]

F. Protections Against Disclosure of Certain Specific Medical Record Information

Certain medical information considered to be particularly sensitive carries heightened legal protection. However, it should be noted that nearly all of the statutes contain language allowing for disclosure if "required" or "authorized" by law, and none of the information is completely shielded from court-ordered disclosure.

Physicians, health care providers and health care facilities are prohibited from "disclos[ing] the results of an [HTLV antibody or antigen] test to any person other than the subject thereof without first obtaining the subject's written informed consent".[54] [55]

Communication between a psychotherapist and a patient are privileged, with six exceptions:[56]

(1) a psychotherapist may reveal patient communications for the purpose of hospitalizing a patient the psychotherapist determines is a danger to himself or others.

(2) a court-appointed psychotherapist may reveal patient communications following a court-ordered evaluation of a patient, provided that the patient had been warned initially that his or her communications would not be privileged.

(3) a psychotherapist may reveal a patient's communications in a proceeding where the patient has put his mental or emotional state at issue as an element of his or her claim or defense (other than in a child custody or adoption matter) and the judge or hearings officer determines that the interests of justice served by disclosure outweigh the value of the privilege.

(4) Same as (3) except after death of patient where the claim is by and on behalf of patient's beneficiaries.

(5) a psychotherapist may reveal a patient communication upon court order in a child custody case.

(6) a psychotherapist may reveal a patient communication in his or her own defense if sued by the patient or subject to malpractice, criminal or license revocation proceedings.[57] [58] [59]

All communications between a victim and a sexual assault counselor are confidential, when made for the purpose of counseling and assistance.[60] In extremely limited circumstances, defendants charged with sexual assault may gain access to the records.[61]

Hospital, dispensary, laboratory and morbidity reports and records pertaining to venereal disease may not be divulged except by court order or by the authority of the Commissioner of Public Health.[62] [63]

The records of alcohol detoxification and treatment facilities are confidential but may be released upon a court order.[64]

The records of facilities for the treatment of drug dependency are confidential except that they must be disclosed upon court order, or when required by federal law.[65]

G. Other Privacy Protections

Massachusetts has a general privacy protection statute which states: "A person shall have a right against unreasonable, substantial, or serious interference with his privacy".[66] This statute has been used by plaintiffs to recover damages for unauthorized release of medical information.[67]

Also, the commonwealth's "Fair Information Practices Act" prohibits the release of "personal data" held by a public agency unless consented to by the subject or pursuant to law, or court order.[68]

IV.

Recommendations

As the preceding survey of the law demonstrates, in comparison to the complaints that have come to the attention of the Attorney General, many aspects of medical information collection and use are not adequately covered by state law with respect to patient confidentiality. There is nothing that governs proper maintenance and management of electronic records, nothing addressing the concern of privacy advocates with respect to genetic discrimination, and nothing effectively regulating marketing of medical information.

In addition, most existing protections require the individual whose privacy has been violated to take action in response, generally by means of a civil suit. This is not a totally effective enforcement mechanism for, as should be obvious, what remains of one's privacy disappears in the course of a lawsuit. Any legislation to enhance privacy protection should, in addition to creating private rights, also vest both civil and, when appropriate, criminal enforcement power in a public authority or authorities able to act in the public interest. This would also create effective enforcement in cases where many minor violations occur which, while not worth pursuing by the individual victims, nonetheless in the aggregate should be stopped.

In light of the developing concern regarding eroding medical privacy the current state of the law, and the basic principles endorsed by the Attorney General, the following are the Attorney General's recommendations for action.

A. Model Security Provisions For the Protection of Electronic Medical Records

Any health care provider who decides to transfer individual medical records to an electronic database should abide by standardized security protections. A number of organizations have already proposed standard policies which at a minimum should include:

1. Strong training and disciplinary policies around proper use of the electronic medical record, including training of the clerical personnel assigned to in-put already existing data into the system and adequate security for paper records during the in-put process.

2. Location of computers with multiple users in secure, visible areas, where an unauthorized user would find access difficult and conspicuous. Automatic log-off of all computers after a defined period without use.

3. Authorization of users by unique identifier passwords, a complete list of which is maintained by the system operator, who should revoke and re-assign them at random but frequent intervals.

4. Regular audit of passwords by the system operator with immediate deletion of a password when the authorized user leaves the job.

5. Installation of layered access programs to insure users have only the level of access to the medical record needed to do their particular job. The access should be set at the least necessary and convenience alone should never outweigh privacy concerns. Log-on screens should remind users of confidentiality policies, including that violation will result in loss of employment.

6. The system should be capable of generating comprehensive audit trails, including the date and time a record is accessed, the password used, which information in the record was reviewed, were any additions or alterations made. It should be possible to generate an audit based on the particular record, the particular user or any other field in the audit. Patients should be able to request an audit. Employees who receive treatment at their employment facility should be able to audit their own records.

7. The system operator should use regular run anti-virus programs. In addition, the system operator should carry out regular security audits of the system on a whole to detect tampering.

8. Highly sensitive information should be maintained at the highest and most restricted levels of access with additional password protection, and should be updated and/or altered only by the patient's physician. Warning screens should precede any access to the information and no print-out should be possible without a screen that again warns of the sensitivity of the information and requests specific authorization and user identification to print.

9. There should be policies addressing remote access points into the medical records database.

10. There should be no transmission of identifiable patient information over the Internet without specific consent by the patient, and the patient should be informed of whatever methods will be used to protect the security of the transmission.

11. Every page of a print-out from the electronic record should contain the name of the person generating the print-out. Printers should be in the immediate proximity of the computer and print-outs should be picked up immediately and incinerated or shredded after use.

12. No more information should be printed out than is necessary for the particular patient contact, e.g. a patient's complete gynecological history should not be

printed out for the physical therapist treating the patient's tennis elbow. Policy should discourage creating unnecessary paper records and, where possible, clinicians should view appropriate patient information on-screen without generating a paper record. Records older than three years should be archived on the system and should not be routinely accessible unless there is a specific clinical reason to do otherwise.

13. There should be adequate back-up of records and planning so that the database is not lost in the event of a disaster.

14. Policies should be adopted and enforced around secure use of fax machines.

15. Discussion of identifiable patients' care over cellular phones should not be a routine practice, but should be limited to urgent situations, and should be avoided if possible.

The Attorney General recommends a statute mandating every holder of an electronic medical record to have standardized security procedures in place.

B. Protecting Against Discrimination On The Basis of Genetics

1. Genetic testing should be prohibited except with the specific informed consent of the patient.

2. The results of genetic testing should not be routinely available to secondary users, such as employers or insurers, and no one should be required to submit to a genetic test in order to obtain employment or health insurance. Discrimination in employment, housing and public accommodation on the basis of genetic testing should be prohibited.

The Attorney General recommends amending G.L. c. 151B to address these concerns.

C. Barriers Between Providers And Commercial Users of Medical Information

1. The barriers between health care providers and commercial users of medical information should be strengthened. Health insurers or HMOs and all other health case providers should be barred from selling or otherwise providing any information to marketers, including mailing lists. The Attorney General recommends that G.L. c. 175I § 13 be amended to prohibit this practice. There should be similar prohibitions against pharmacists selling or otherwise providing the information as well, and a new statute should be provided for that purpose.

2. Any direct mail marketing of medical products directly to consumers should identify the source from which the mailing list was derived, so that consumers can be assured that their medical information is not being sold for commercial gain by their health care providers or insurers. The Attorney General recommends a new statute for this purpose.

D. Getting Control of the Government's Demand For Medical Information/Encouraging Public Attention/Informed Consent

In addition, to the specific issues above, there is a more general concern that needs to be addressed. When considering future laws that grant access by secondary users to identifiable medical information without consent, more attention should be given to weighing the potential benefits arising from the use against the detriment to privacy concerns. Some of the issues raised can be more subtle than a surface review may suggest. For example, proponents of increased access to identifiable patient information without a specific consent to disclose from the patient often point to medical research as an area where the benefits clearly outweigh the privacy interest. They note, correctly, that society as a whole benefits enormously from medical research, which in turn benefits enormously from unfettered access to relevant data.

Undoubtedly, requiring informed disclosure does create burdens on research. First, there is an administrative cost to obtaining the consents, both financially and in terms of time. Also, there are at least some indications that a large majority of patients will, when asked, consent to the use of their medical information for research purposes,[69] so a formal request for a consent begins to appear unnecessary, even from the privacy protection standpoint. Second, if a small percentage of patients do refuse consent potentially valuable information is being kept from the researchers and the result can be skewed or ineffective studies. Should individual preferences for privacy be allowed to outweigh the social benefit of fully informed medical research?

The Attorney General suggests that this question raises, in an unusual guise, the basic issue of a democratic society. When should the government require the surrender of a individual right for a defined "greater" good? Who decides that the good is, in fact "greater"? (Not all medical research is well-designed or extremely valuable.) Is the additional expense of requiring researchers to obtain consented to disclosure a reasonable cost for the society to bear in balancing the public versus the private interest? If most citizens choose willingly to give up their privacy as a matter of civic responsibility, should government take this as permission to deny them the choice? Should those that are less sensitive to privacy concerns set the standard for those who are more sensitive to them?

These are questions that require a more open debate. Although the issue of medical privacy has been an active topic among privacy advocates, health care professionals and information management specialists, to date the general public has not had much input. Most experts have simply assumed that a centralized medical information

system would be seen by the public as primarily benefiting their care. However, as noted above, this is only part of the privacy concern and perhaps the easiest one to make assumptions about. The Attorney General would like to encourage more input from the general public, and recommends:

1. Surveys by both the government and the other collectors of health information of the patient's view of privacy and access to their records.

2. Public debate and/or hearings on any legislation that increases access to medical records or increases reporting requirements, to determine in all cases whether the legislation is necessary and, if it is, the least amount of intrusion necessary to accomplish the result.

Finally, the Attorney General does not view "informed consent" provisions as a means to protect patient privacy in a meaningful way. Indeed, "informed consent" as a concept is misapplied and confusing in this context. "Informed consent" generally refers to a physician's obligation to disclose in a reasonable manner all significant medical information that is material to an intelligent decision by a patient whether to undergo a proposed procedure.[70] While it may be possible for a provider of medical care to completely disclose to a patient how the patient's information will be gathered, stored, distributed and used, it is realistically never possible for the patient to make a decision to decline to provide the information if the patient wants any medical treatment at all. It is hard to imagine a provider agreeing to provide treatment to a patient who, upon hearing what the provider intends to do with his medical information, declines to give it to the provider. In reality, the emphasis should be on "full disclosure," not spurious "informed consent." Where the consumer is forced to choose between surrendering privacy or forgoing health care, no amount of prior explanation as to exactly how the private medical information is to be disseminated makes the "consent" any less coerced.

However, there is a value to the suggestion that consumers be fully informed of how their records are used by their health care providers. Providing detailed information to consumers is the best way to ensure public awareness of the altered use of medical information and to encourage their participation in setting appropriate boundaries and rules around the use of the information. It will make it plain to consumers that, at present, the only genuine power they have to protect their medical privacy comes at a socially and medically unacceptable cost – to withhold information from their health care providers or to ask their providers not to record the information. It will make explicit what has, to date, occurred without much knowledge by the public, the fact that medical privacy is diminishing, and its loss has real consequences both for individuals seeking treatment and the system as a whole.

CONCLUSION

While there is no doubt that new information technologies can offer significant health care benefits, the processes must be carefully monitored to insure the benefits do not come at the expense of personal privacy. This report is offered in furtherance of that goal. The Attorney General hopes that this report will contribute to public awareness and discussion of the issues raised and will encourage the efforts that others are making in this direction.

ENDNOTES

[1] The Attorney General would like to acknowledge the assistance of the Medical Records Department Staff at the Brigham and Women's Hospital, the Visiting Nurses Association, Blue Cross/Blue Shield and Harvard Pilgrim Health Plan in providing background information for this report.

[2] G.L. c. 111 § 70. See also 243 C.M.R. 2.07 (13), which requires all physicians licensed in the commonwealth to maintain records.

[3] Alberts v. Devine, 395 Mass. 59 (1985). P.J. Liacos, Massachusetts Evidence, 186-188, (5th ed. 1981). "The principle that society is entitled to every person's evidence in order that the truth may be discovered, may require a physician to testify in court about information that may be obtained from a patient in the course of treatment." Alberts at 67.

[4] Bratt v. IBM, 392 Mass. 508, 523 (1984).

[5] Alberts, supra at 68.

[6] It should be emphasized that the ethical/legal obligation of confidentiality is generally contingent on the establishment of a doctor-patient relationship. Where a person provides information to a doctor when not a patient of the doctor, confidentiality restrictions do not necessarily apply. For example, a doctor examining a person on behalf of a potential employer or an insurance company is not bound to keep the person's communications confidential, but may provide the information to the employer or the company. However, the Supreme Judicial Court has found that a non-treating psychiatrist, retained as an expert witness in a child custody dispute on behalf of mother who was alleging sexual abuse of the child by the father, acted in violation of the family's privacy when she released medical information in the case to a reporter. Sugarman v. Board of Registration in Medicine, 422 Mass. 338 (1996).

[7] G.L. c. 111, § 70E.

[8] [A]ny hospital, institution for the care of unwed mothers, clinic, infirmary maintained in a town, convalescent or nursing home, rest home, or charitable home for the aged, licensed or subject to licensing by the department; any state hospital operated by the department; any "facility" as defined in section three of chapter one hundred and eleven B; any private, county or municipal facility, department or ward which is licensed or subject to licensing by the department of mental health pursuant to section nineteen of chapter nineteen; or by the department of mental retardation pursuant to section fifteen of chapter nineteen B; and "facility" as defined in section one of chapter one hundred and twenty-three; the Soldiers Home in Holyoke, the Soldiers' Home in Massachusetts; and any facility set forth in section one of chapter nineteen or section one of chapter nineteen B.

[9] G.L. c. 231, § 60B-E.

[10] This, however, is not a practical remedy for a confidentiality violation standing alone, as it requires the claimant to satisfy all the prerequisites to a malpractice action, including undergoing review by a tribunal.

[11] Pursuant to G.L. c. 111, § 70.

[12] G.L.c. 111 § 70E, G.L.c. 111§ 70.

[13] Pursuant to G.L. c. 111 § 70E. Also, the American Health Information Management Association has mandated standards for making changes in medical records which have been adopted by most Massachusetts hospitals.

[14] G.L. c. 112 § 12CC.

[15] G.L. c. 208 § 31, G.L. c. 112 § 12S.

[16] G.L. c. 201D § 5.

[17] G.L. c. 112 § 12F.

[18] G.L. c. 201D § 5.

[19] G.L. c. 111 § 70F.

[20] H. 52 filed January, 1997.

[21] Authorizations by federal law are also numerous, but beyond the scope of this report.

[22] G.L. c. 111 § 70. See, also G.L. c. 233 § 7a, admissibility of medical records in court.

[23] G.L. c. 123 § 36A, 104 C.M.R. 2.07.

[24] G.L. c. 111 § 70.

[25] G.L. c. 111 § 24A.

[26] G.L. c. 152 § 30A.

[27] Holders of this information consider that the provisions of G.L.c. 111 § 70 (which prohibit disclosure of medical information without patient consent) override this requirement, due to that statute's narrower and more specific prohibitory language.

[28] G.L. c. 111 § 6; 105 C.M.R. 300.

[29] G.L. c. 112 § 12A.

[30] G.L. c. 119 § 51A.

[31] G.L. c. 19A § 15.

[32] G.L. c. 19A §§ 30, 31.

[33] G.L. c. 111 § 111B.

[34] G.L. c. 111 § 67A.

[35] G.L. c. 46 § 3A.

[36] G.L. c. 46 § 9; G.L. c. 111 § 24B.

[37] G.L. c. 111 § 202.

[38] G.L. c. 111 § 110B.

[39] G.L. c. 111 § 111A.

[40] G.L. c. 111 § 191.

[41] G.L. c. 111 § 72G.

[42] G.L. c. 111 § 111C (the "Ryan White" Act). See 105 C.M.R. 172, defining those diseases for this purpose as infectious tuberculosis, measles, mumps, rubella, chickenpox, hepatitis B, HIV infection/AIDS, hepatitis C, diphtheria, meningococcal disease, plague, hemorrhagic fever (e.g. Ebola) and rabies.

[43] G.L. c. 111 § 70A-D.

[44] G.L. c. 112 § 12G.

[45] G.L. c. 111 § 6D.

[46] G.L. c. 152 § 20A.

[47] G.L. c. 111 § 70E. ["No provision of this section relating to confidentiality of records shall be construed to prevent any third party reimburser from inspecting and copying in the ordinary course of determining eligibility for benefits any and all records relating to diagnosis, treatment, or other services provided to any person including a minor or incompetent, for which coverage, benefit or reimbursement is claimed, so long as the policy or certificate under which the claim is made provides that such access to such records is permitted."]

[48] G.L. c. 175I § 13.

[49] The Medical Information Bureau, Inc. (MIB) is a trade association of 680 life insurance companies, including virtually every major issue of life, health and disability insurance in the U.S. It was established in 1902 as a fraud detection and prevention service. MIB collects individually identifiable medical information on insurance applicants. It now has a database of approximately 15 million individuals and provides information in coded form upon request to member companies over a network of approximately 1,000 dedicated computer terminals.

[50] G.L. c. 111 § 70E.

[51] G.L. c. 111 § 204.

[52] G.L. c. 111 § 205. The Board of Registration in Medicine has subpoena power pursuant to G.L. c. 112 § 5. Incident reports and certain other records of a peer review committee that may contain information about individual patients, are, if necessary for the work of the peer review committee, confidential, and cannot be disclosed except to the Board of Registration in Medicine.

[53] G.L. c. 111 § 205.

[54] G.L. c. 111 § 70F.

[55] While this appears to be an absolute prohibition, note that it applies only to test results, and not to other information diagnostic of AIDS. See also G.L. c. 123 § 3 6, re-enacted after G.L. c. 111 § 70F, which authorizes the Commissioner of Mental Health to permit inspection or disclosure of DMH-maintained medical records at the Commissioner's discretion, when in the best interest of the patient, "notwithstanding any other provision of law."

[56] G.L. c. 233 § 20B and 20J.

[57] See also, Commonwealth v. Kobrin, 395 Mass. 284 n.18 (1985) limiting the privilege to "communications" and holding that "observations of objective indicia of emotional disturbance [such as] disturbance of sleep or appetite; anergia; impaired concentration or memory; hopelessness; anxiety or panic; dissociative states; hallucinations; labile or flattened affect; or somatic symptoms such as headaches" may be released.

[58] G.L. c. 112 § 128A. Creates substantially the same privilege for psychologist-patient communication.

[59] G.L. c. 112 § 135A. Creates substantially the same privilege for social worker-client communication.

[60] G.L. c. 233 § 20J.

[61] Comm. v. Fuller, 423 Mass. 216 (1996); Comm. v. Bishop, 416 Mass. 169 (1993). (See also G.L. c. 112 § 12A1/2, which requires physicians to report rapes and sexual assaults to local police and the criminal history systems board, but which prohibits including "patient identifiers" in the report.)

[62] G.L. c. 111 § 119.

[63] But see, G. L. 112 § 12 which permits a physician to disclose without consent a diagnosis of venereal disease to a person who has given "a promise of marriage" to the patient. If given in good faith, the information may not be the basis of a slander or libel claim against the doctor, although the statute makes no reference to liability for invasion of privacy.

[64] G.L. c. 11B § 111.

[65] G.L. c. 11E § 18.

[66] G.L. c. 214 § 1B.

[67] Tower v Hirschhorn, 397 Mass. 581 (1986). Bratt v IBM, 392 Mass. 508 (1984).

[68] G.L. c. 66A § 2.

[69] See, e.g. L. Joseph Melton III, M.D., "The Threat to Medical Record Research," The New England Journal of Medicine, 337 (1997): 1466-69.

[70] Harnish v. Children's Hospital Medical Center, 387 Mass. 152 (1982).